509,296

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

Rec'd PCT/PTO 24 SEP 2004

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
2 octobre 2003 (02.10.2003)

PCT

(10) Numéro de publication internationale
WO 03/081547 A1

(51) Classification internationale des brevets[7] :
G07F 19/00, G06F 17/60

(21) Numéro de la demande internationale :
PCT/FR03/00937

(22) Date de dépôt international : 25 mars 2003 (25.03.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :
02/03678 25 mars 2002 (25.03.2002) FR

(71) Déposant *(pour tous les États désignés sauf US)* : **FRANCE TELECOM** [FR/FR]; 6 Place d'Alleray, F-75015 PARIS (FR).

(72) Inventeurs; et
(75) Inventeurs/Déposants *(pour US seulement)* : **PETIT, Stéphane** [FR/FR]; 68, rue Hébert, F-14200 Hérouville Saint Clair (FR). **VALLEE, Françoise** [FR/FR]; 48, rue Fleurie, F-14480 Lantheuil (FR).

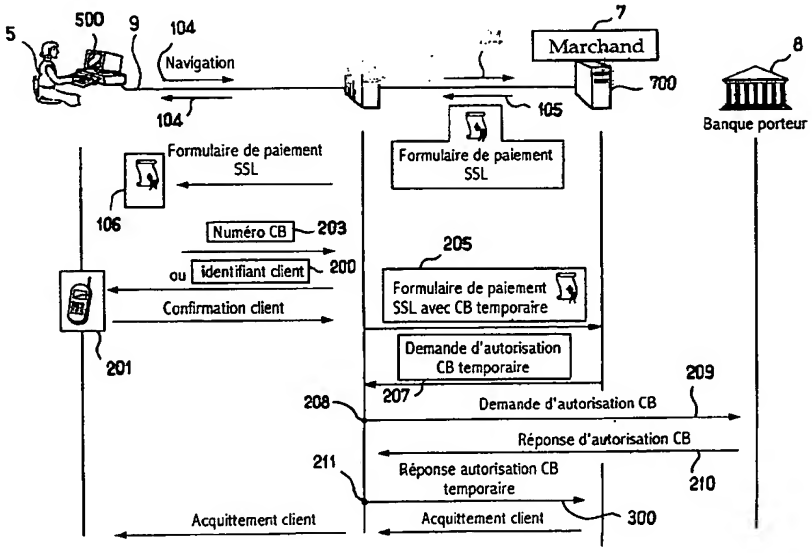
(74) Mandataires : **MARTIN, Jean-Jacques** etc.; Cabinet Regimbeau, 20, rue de Chazelles, F-75847 Paris Cedex 17 (FR).

(81) États désignés *(national)* : AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ,

[Suite sur la page suivante]

(54) Title: METHOD AND SYSTEM OF SECURING A CREDIT CARD PAYMENT

(54) Titre : PROCEDE ET SYST[illegible]ECURISATION D'UN PAIEMENT PAR CARTE DE CREDIT



1 BROWSING
2 PAYMENT FORM
3 BC NUMBER
4 CUSTOMER IDENTIFIER
5 OR
6 CUSTOMER CONFIRMATION
7 CUSTOMER ACKNOWLEDGEMENT
8 THIRD PARTY
9 PAYMENT FORM
10 PAYMENT FORM SSL WITH TEMPORARY BC
11 TEMPORARY BC AUTHORISATION REQUEST
12 BC AUTHORISATION REQUEST
13 BC AUTHORISATION RESPONSE
14 TEMPORARY BC AUTHORISATION RESPONSE
15 CUSTOMER ACKNOWLEDGEMENT
16 CARD HOLDER BANK
17 MERCHANT

(57) **Abstract:** The invention relates to a method of securing credit card transactions between a credit card holder (5) and a merchant (7), e.g. via a telecommunication network (9). The invention is characterised in that it comprises the following steps: the holder (5) informs a third party (6) of his/her intention to contact the merchant (7); the holder (5) contacts the merchant (7) through the intermediary of the third party; the third party (6) establishes a connection with the holder (5) and establishes a connection with the merchant (7); and the third party (6) manages the formation of temporary information, the inputting of said information into the order form and the relational linking of the temporary information with the card holder's actual bank information in order to check the different authorisations in relation to the banks for the acknowledgement of the order. The invention also relates to a system using said method.

(57) **Abrégé :** L'invention concerne un procédé de sécurisation de transactions par carte de crédit entre un porteur (5) et un marchand (7), notamment à travers un réseau de télécommunication (9), caractérisé en ce qu'il comporte les étapes selon lesquelles le porteur (5) signifie à un tiers (6) son intention d'entrer en

[Suite sur la page suivante]

WO 03/081547 A1

DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) **États désignés** *(régional)* : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclaration en vertu de la règle 4.17 :

— *relative à la qualité d'inventeur (règle 4.17.iv)) pour US seulement*

Publiée :

— *avec rapport de recherche internationale*

— *avant l'expiration du délai prévu pour la modification des revendications, sera republiée si des modifications sont reçues*

En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.

contact avec le marchand (7) ; le porteur (5) entre en contact avec le marchand (7) par l'intermédiaire du tiers ; le tiers (6) établit une liaison entre lui et le porteur (5), ainsi qu'entre lui et le marchand (7) ; le tiers (6) gère la formation d'informations temporaires, l'entrée de ces informations dans le formulaire de commande ainsi que la mise en relation des informations temporaires et des véritables informations bancaires de la carte de crédit du porteur pour contrôler les différentes autorisations auprès des banques pour l'acquittement de la commande. L'invention concerne également un système de mise en ceuvre du procédé.

PROCEDE ET SYSTEME DE SECURISATION D'UN PAIEMENT PAR CARTE DE CREDIT

DOMAINE TECHNIQUE GENERAL

La présente invention concerne un procédé de sécurisation de transaction par carte de crédit, notamment à travers un réseau de télécommunication.

Plus précisément, elle concerne une sécurisation de transaction par carte de crédit entre un porteur et un marchand, cette transaction s'effectuant sur un réseau de télécommunication ou vente à distance.

Elle s'applique notamment, mais non limitativement, au domaine du paiement par procédure du type vente à distance sur Internet.

On appelle dans la présente demande carte de crédit tout type de carte, de crédit à proprement parler, mais également les carte de paiement et de retrait, du type carte bancaire.

ETAT DE L'ART.

On rappelle que les cartes bancaires et/ou de crédit [illegible] d'une part une partie visuelle, et d'autre part une piste magnétique, ainsi qu'une puce dans certains pays, ces trois parties intégrant des informations sur le porteur.

Les informations reportées sur la partie visuelle sont par exemple le nom et le prénom du porteur, ainsi que des informations d'identification bancaire de la carte elle-même, notamment le numéro de la carte bancaire ainsi que la date d'expiration de sa validité. La partie visuelle de la carte peut éventuellement comporter une signature manuelle du porteur.

La piste magnétique, et la carte à puce le cas échéant, reprennent les informations précédentes ainsi que des informations complémentaires, dont le code confidentiel lié à la carte bancaire (présent de façon chiffrée).

Il est possible d'effectuer des transactions financières avec de telles cartes de crédit.

Plusieurs procédures de transactions financières sont possibles.

Pour effectuer une transaction bancaire ou financière, on peut, selon une première possibilité, n'utiliser que les informations contenues dans la partie visuelle de la carte. Cette procédure est qualifiée de procédure vente à distance.

Seules les informations contenues dans la partie visuelle sont nécessaires pour valider la transaction financière.

Cette procédure est couramment utilisée sur les réseaux de télécommunication, par exemple Internet, mais également dans le cadre du commerce à distance, comme la vente par correspondance par exemple, ces ventes pouvant s'effectuer à l'aide de téléphones.

La seconde possibilité utilise les informations contenues sur la piste magnétique pour effectuer une transaction financière. Pour valider la transaction financière, un automate situé chez le marchand comporte des moyens aptes à lire les informations présentées sur la partie magnétique de la carte. Une signature manuelle du porteur en face du marchand permet d'identifier localement le porteur.

Cette dernière procédure est utilisée hors de France.

Cependant, le fait que seule une signature manuelle soit nécessaire à la validation de la transaction engendre des taux de fraude relativement importants.

La France a décidé d'utiliser une méthode plus sûre pour effectuer les transactions par carte de crédit. Elle utilise notamment une carte à puce.

La carte à puce a la capacité d'une part, d'authentifier à chaque transaction financière du porteur de la carte de crédit par présentation et vérification locale du code confidentiel, et, d'autre part, de générer des preuves sur l'acte d'achat à l'aide des secrets personnalisés qu'elle contient.

De telles transactions nécessitent l'emploi d'automates spécifiques chez le marchand. Ces automates contiennent notamment des moyens aptes à lire la carte à puce.

Pour sécuriser les transactions financières effectuées lors du commerce sur un réseau de télécommunication, il suffirait d'utiliser la même méthode. Cependant, il est difficile de mettre à disposition de chaque utilisateur sur le réseau un automate ayant des moyens de lecture de carte à puce.

De plus, comme la France est un des rares pays à l'heure actuelle à utiliser la sécurisation par carte à puce, une telle fourniture de moyens ne permettrait que d'effectuer des transactions entre des porteurs français et des commerçants ou marchands français.

Par conséquent, les transactions financières sur réseaux de télécommunication utilisent toujours les méthodes utilisants les parties visuelles de la carte de crédit.

La facilité avec laquelle les parties visuelles sont fraudables (par génération informatique de numéros de cartes, ou par vol) font que les taux de fraude sur le commerce par réseau de télécommunication sont très élevés.

Plusieurs [illegible] visant à sécuriser de telles transactions sont déjà connues.

Elles préconisent la non circulation du numéro de carte du porteur sur le réseau de télécommunication.

Une première méthode consiste à utiliser des plates-formes de commerce électronique, qui proposent au porteur d'inscrire définitivement leur numéro de carte sur leur serveur et d'utiliser un pseudonyme (comme un mot de passe, un mot de connexion, parfois un questionnaire complémentaire) pour effectuer les transactions financières.

Les informations bancaires du porteur ne circulent plus sur le réseau, et le marchand devra effectuer un certain nombre d'opérations pour obtenir les informations nécessaires à la validation de la transaction.

Une deuxième méthode substitue au réel numéro de carte bancaire du porteur un numéro temporaire parfaitement formé. Le porteur collecte auprès d'un centre d'autorisation spécialisé une série de numéros de cartes temporaires qui seront utilisés par le porteur pour acheter des

produits ou des services auprès du marchand lors d'une transaction sur le réseau de télécommunication.

Un centre d'autorisation de la transaction collecte ensuite les transactions financières associées à un numéro temporaire, remplace le numéro temporaire par le vrai numéro de la carte bancaire et renvoie la transaction financière vers un véritable centre d'autorisation des transactions financières de la banque du porteur.

Ces procédés de sécurisation du commerce sur réseau de télécommunication présentent cependant des inconvénients.

Le premier procédé ne permet d'effectuer des opérations financières qu'avec une population fermée de marchands.

Le deuxième procédé nécessite l'installation de moyens spécifiques (comme par exemple un « wallet » ou paquet de numéros temporaires de carte parfaitement formés) sur le poste de communication du porteur. Ces moyens sont liés au poste du porteur, et ce dernier ne peut pas effectuer de commerce sécurisé à partir d'un autre poste de navigation sur le réseau.

Enfin, il doit effectuer des manipulations pour remplir le bon de commande du marchand à l'aide des numéros de cartes bancaires temporaires.

PRESENTATION DE L'INVENTION.

L'invention propose de pallier ces inconvénients.

L'invention a notamment pour but de permettre à un utilisateur de pouvoir effectuer une transaction par carte bancaire sur le réseau de communication qui soit sécurisée, cette transaction pouvant s'effectuer à partir de n'importe quel terminal de communication.

Le terminal de communication pourra par exemple être un poste de navigation, ou par exemple un téléphone mobile.

L'invention consiste à éviter la circulation, sur le réseau et en direction du marchand, d'informations bancaires concernant la carte de crédit du porteur.

L'invention a également pour but de minimiser au minimum l'intervention du tiers dans la gestion de la transaction, et notamment dans la saisie des différents numéros temporaires de carte de crédit par exemple.

A cet effet, l'invention propose un procédé de sécurisation de transactions par carte de crédit entre un porteur et un marchand, notamment à travers un réseau de télécommunication, en entrant dans le formulaire de commande fourni par le marchand, lors de la phase de paiement de la transaction, des informations temporaires cohérentes avec les informations bancaires de la carte du porteur, ces informations temporaires étant ensuite collectées par un centre d'autorisation de la transaction afin d'être mises en relation avec les véritables informations bancaires de la carte du porteur pour l'acquittement de la commande par le porteur au bénéfice du marchand, caractérisé en ce qu'il comporte les étapes selon lesquelles :

- le porteur signifie à un tiers son intention d'entrer en contact avec le marchand ;
- le porteur entre en contact avec le marchand par l'intermédiaire du tiers ;
- le tiers établit une liaison entre lui et le porteur, ainsi qu'entre lui et le marchand ;

le tiers gère la formation d'informations temporaires, l'entrée de ces informations dans le formulaire de commande ainsi que la mise en relation des informations temporaires et des véritables informations bancaires de la carte de crédit du porteur pour contrôler les différentes autorisations auprès des banques pour l'acquittement de la commande.

L'invention est avantageusement complétée par les caractéristiques suivantes, prises seules ou en une quelconque de leur combinaison techniquement possible :

- la liaison entre le tiers et le porteur est sécurisée de façon à permettre au tiers d'intercepter et de contrôler toutes les informations transmises par le porteur en direction du marchand via le tiers, mais de façon transparente pour le porteur ;
- la liaison entre le tiers et le marchand est sécurisée de façon à permettre au tiers d'intercepter et de contrôler toutes les informations transmises par

le marchand en direction du porteur via le tiers, mais de façon transparente pour le porteur ;

- le porteur signifie son intention d'entrer en contact avec le marchand en effectuant une connexion sur le site du tiers et/ou en indiquant l'adresse Internet - ou « Uniform Resource Locator » (URL) selon la terminologie anglo-saxonne généralement utilisée - du tiers dans un navigateur de réseau de télécommunication ;
- le site du tiers est du type Espace de Commerce Sécurisé – ou « Secure Commerce Space » (SCS) selon la terminologie anglo-saxonne généralement utilisée -,
- la liaison sécurisée entre le porteur et le tiers peut être du type Couche d'interface de connexion sécurisée ou « Secure Socket Layer » (SSL) selon la terminologie anglo-saxonne généralement utilisée ;
- la liaison sécurisée entre le tiers et le marchand peut être du type Secure Socket Layer ;
- le tiers modifie les adresses Uniform Resource Locator relatives ou absolues du site du marchand pour contraindre le navigateur du porteur à transmettre systématiquement audit tiers toutes les informations en provenance du porteur vers le marchand, ainsi que celles en provenance du marchand vers le porteur ;
- le tiers modifie les adresses Uniform Resource Locator relatives ou absolues du site du marchand pour contraindre le navigateur du marchand à transmettre systématiquement audit tiers toutes les informations en provenance du marchand vers le porteur, ainsi que celles en provenance du marchand vers le porteur ;
- deux procédures d'acquittement de la commande sont possibles en fonction de l'inscription préalable ou non du porteur auprès du tiers, cette inscription comprenant la transmission audit tiers des informations bancaires concernant le porteur et sa carte de crédit dans un registre du tiers ;
- si le porteur s'est préalablement inscrit auprès du tiers, il peut choisir de ne pas indiquer dans le domaine réservé du bon de commande de la transaction les informations bancaires le concernant, et par conséquent ne

remplir ledit domaine que par un identifiant auprès du tiers, le remplissage de la partie nécessitant des informations bancaires étant effectué par le tiers avec des informations temporaires et cohérentes, seules ces informations temporaires étant envoyées au marchand ;

- on déclenche une procédure de vérification de la volonté du porteur d'effectuer la transaction ;
- la vérification comporte une étape selon laquelle on rappelle le porteur sur son téléphone mobile, le porteur signifiant son accord au tiers par la saisie d'un mot de passe qui peut être renvoyé grâce à un Short Message Service, et/ou une signature électronique générée par le téléphone mobile ;
- la vérification comporte une étape selon laquelle le porteur saisit dans une fenêtre sécurisée un mot de passe sur les moyens connectés au réseau de télécommunication ;
- la vérification comporte une étape selon laquelle on envoie un courrier électronique au porteur, le porteur devant alors renvoyer le courrier électronique avec un [illegible] permettant de confirmer la transaction ;
- la vérification comporte une étape selon laquelle on vérifie la signature cryptographique de moyens que le porteur a en sa possession, notamment une carte à puce introduite dans un lecteur relié au réseau de télécommunication ;
- dans le cas où le porteur n'est pas inscrit auprès du tiers, il entre les informations bancaires de sa carte de crédit dans le formulaire de commande fourni par le marchand via le tiers, le tiers gérant alors le remplissage du formulaire de commande qui sera envoyé au marchand avec des informations temporaires ;
- il comporte les étapes selon lesquelles :
  - un centre d'autorisation bancaire relié au tiers collecte la demande d'autorisation bancaire en provenance du marchand ou de sa banque et contenant les informations temporaires ;
  - le centre effectue une reconversion mettant en relation les informations temporaires et les véritables informations bancaires ;

- il envoie les véritables informations bancaires du porteur au centre d'autorisation bancaire du porteur ;
- il récupère la réponse en provenance du centre d'autorisation bancaire du porteur contenant les véritables informations bancaires ;
- il effectue une reconversion pour mettre à nouveau en relation les véritables informations bancaires et les informations temporaires ;
- il renvoie au marchand ou au centre d'autorisation de sa banque la réponse du centre d'autorisation bancaire du porteur contenant les informations temporaires.

- périodiquement, le centre de collecte des transactions du marchand envoie l'ensemble des transactions passées entre ledit marchand et des porteurs par l'intermédiaire du tiers vers un centre de collecte lié au tiers, le tiers effectuant de nouveau une reconversion des informations temporaires en véritables informations bancaires des différents porteurs, le centre de collecte lié au tiers effectuant alors la redistribution des transactions vers les différents centres de collecte des banques des porteurs.
- le centre d'autorisation du porteur comporte en outre un module Profil du Client en Banque (PCB) qui reçoit, par une liaison sécurisée, les demandes d'autorisation bancaire issues du centre d'autorisation relié au tiers, ce module étant configuré par le centre de demande d'autorisation relié au tiers pour qu'il donne au centre d'autorisation du porteur des informations pour le déblocage, transaction par transaction, d'une interdiction d'acquittement des transactions effectuées par le porteur directement par réseau de télécommunication ; et
- les informations bancaires sont le numéro et de la date d'expiration de validité de la carte de crédit.

L'invention concerne également un système permettant la mise en œuvre du procédé selon l'invention.

Par conséquent, l'invention ne nécessite pas d'installation de matériel spécifique de la part du porteur.

Ainsi, l'utilisation du procédé n'est pas lié au poste ou aux moyens liés au porteur.

Le procédé augmente la sécurisation des transactions financières sur réseau de télécommunication, notamment Internet, en évitant que le marchand, ou toute autre personne présente sur le réseau n'ait accès au informations bancaires de la carte de crédit du porteur.

Le procédé peut être associé aux applications de la banque à domicile.

Enfin, le procédé de sécurisation est compatible avec l'ensemble des sites marchands présents sur le réseau de télécommunication.

Le procédé peut avantageusement être complété en permettant à la banque du porteur :

- d'offrir des crédits en ligne lorsque le montant de la transaction s'avère important,
- de développer une véritable relation client en instituant le passage par la banque à domicile (mise à disposition d'informations sur la banque par exemple),
-de gérer d'autres produits liés au paiement pour le client (paiement différé par exemple, ouverture d'un compte spécialisé Internet, etc.).

PRESENTATION DES FIGURES.

D'autres caractéristiques, buts et avantages de l'invention ressortiront de la description qui suit qui est purement illustrative et non limitative et qui doit être lue en regard des dessins annexés sur lesquels :

- La figure 1 représente suivant une présentation schéma-blocs les étapes principales de traitement d'une transaction financière entre un marchand et un porteur ;
- La figure 2 représente sous forme de schéma-blocs les différentes étapes successives selon la première étape principale de la figure 1 ;
- La figure 3 représente sous forme de schéma-blocs les différentes étapes successives de la deuxième étape principale de la figure 1 ;
- La figure 4 représente ce schéma-blocs des différentes étapes successives de la troisième étape principale selon la figure 1 de la transaction financière ;

- La figure 5 représente sous forme de schéma-blocs les étapes successives de la collecte des transactions, cette collecte étant faite périodiquement ;
- La figure 6 représente schématiquement les allers et retours des différentes étapes entre le porteur, le tiers et le marchand ;
- La figure 7 représente schématiquement le système et les transactions permettant de mettre en œuvre le procédé selon la figure 1 ;
- La figure 8 représente schématiquement les différentes transactions bancaires lors d'une transaction financière, notamment réalisée avec un procédé selon une variante de l'invention.

DESCRIPTION DETAILLEE DE L'INVENTION.

En faisant référence aux figures 1 et 6, un porteur 5 souhaite réaliser une transaction financière avec un marchand 7 sur un réseau de télécommunication 9.

La figure 1 montre que cette transaction financière comporte une première étape 1 de commande d'un produit chez le marchand 7, suivie d'une étape 2 de paiement. Le paiement est lui-même suivi d'une étape de livraison 3, suivie, mais pas forcément de façon corrélée, par une étape 4 de collecte de l'ensemble des transactions financières passées par le marchand 7 avec les différents porteur 5 sur un réseau de télécommunication 9.

Le réseau de télécommunication peut être par exemple Internet, mais il peut également s'agir d'un réseau de téléphonie mobile par exemple.

La figure 2 décompose la première phase de la transaction financière, à savoir la phase de commande d'un produit chez un marchand 7, et présente de façon linéaire les différentes étapes successives.

Selon une première étape 100, le porteur 5 indique à un tiers 6 son intention d'effectuer une transaction financière et la commande d'un produit auprès d'un marchand 7. Cette transaction financière est effectuée sur un réseau de télécommunication 9.

Le tiers 6 est présent sur un espace du type Espace de Commerce Sécurisé, ou « Secure Commerce Space » selon la terminologie anglo-saxonne généralement utilisée.

Le tiers 6 peut être un serveur de type « Web » (selon la terminologie anglo-saxonne généralement utilisée) ou Internet intermédiaire, ou tout équipement réseau quelconque.

L'étape 100 consiste donc pour le porteur 5 à se connecter sur le site du tiers sur le réseau 9 de télécommunication.

A cet effet, le porteur 5 possède des moyens 500 – visibles à la figure 6 - permettant la navigation et la connexion sur le réseau 9 de télécommunication, par exemple du type Internet. Les moyens 500 peuvent donc à cet effet comporter un terminal de télécommunication du type micro-ordinateur, ou un téléphone mobile permettant la navigation sur un réseau de télécommunication.

L'étape 101, subséquente à l'étape 100, voit le tiers 6 établir, grâce à des moyens 600, une liaison avec le porteur 5. Le type de liaison dépend du terminal à partir duquel la transaction financière est effectuée.

Dans le cas d'un terminal du type micro-ordinateur permettant une liaison sur Internet, la liaison [illegible] avantageusement une liaison du type Couche d'interface de [illegible]risée ou « Secure Socket Layer » selon la terminologie anglo-saxonne généralement utilisée (ou SSL comme indiqué sur la figure 6).

Grâce à cette liaison, un déroutage effectué par le tiers 6 est possible et permet d'intercepter et de contrôler toutes les informations en provenance des moyens 500 du porteur vers le réseau 9 de télécommunication.

Dans le cas d'un terminal de télécommunication comportant un téléphone mobile, la liaison n'est pas une liaison sécurisée par un moyen SSL.

A l'étape 102, le porteur 5 indique avec quel marchand 7 il veut effectuer une commande et par conséquent éventuellement établir une transaction bancaire. Cette indication s'effectue en saisissant sur ces moyens 500 l'adresse du marchand7 sur le site du tiers 6 sur le réseau. Dans le cas d'Internet il s'agit de l'adresse Internet ou « Uniform Resource Locator » (URL) - selon la terminologie anglo-saxonne généralement utilisée - du marchand.

A partir de cette saisie et de la validation de cette saisie, l'étape 103 consiste pour le tiers 6 à décapsuler informatiquement grâce aux moyens 600 la page ou le site du marchand 7 sur le réseau de télécommunication 9, afin d'établir une liaison éventuellement sécurisée également entre le tiers 6 et le marchand 7. Cette liaison sécurisée est également avantageusement du type Secure Socket Layer (SSL) dans le cas du commerce sur Internet. La décision de sécuriser les échanges par une liaison SSL appartient au marchand 7.

Pour établir une liaison sécurisée, le tiers 6 modifie les adresses Uniform Resource Locator (URL) relatives ou absolues du site du marchand 7 sur le réseau de télécommunication, pour contraindre le navigateur du porteur 5 (compris dans les moyens 500) à transmettre systématiquement audit tiers 6 toutes informations en provenance du marchand vers le porteur 5, et du porteur 5 vers le marchand 7.

A la fin de l'étape 103, toutes les transactions entre le porteur 5 et le marchand sont donc contrôlées par le tiers 6.

Cependant, cette omniprésence du tiers 6 lors du transfert des informations entre le porteur 5 et le marchand 7 est totalement transparente pour le porteur 5, ainsi que pour le marchand 7.

Le porteur 5 navigue sur le réseau de télécommunication 9 ainsi que sur la page du marchand 7 de la même façon que si le tiers 6 n'avait pas le contrôle total du transfert des informations entre les deux parties 5 et 7.

L'étape 104 consiste donc pour le porteur 5 à naviguer sur le site du marchand 7 et choisir un produit qu'il désire acheter.

L'étape 105 correspond à la fin du choix du porteur 5 sur un produit qu'il désire acheter et à l'émission par le marchand d'un bon de commande ou de paiement à remplir par le porteur 5.

Le bon de commande est transmis au porteur 5 à l'étape 106.

La transmission se fait via le tiers 6, ce que soulignent les traits pointillés sur la figure 2 entre les étapes 105 et 106.

L'étape 106 consiste donc pour le porteur 5 à remplir le bon de commande. Ce bon de commande nécessite le remplissage de plusieurs champs, notamment des renseignements sur les coordonnées physiques

du porteur 5 aux fins de livraison du produit, ainsi que des champs concernant les informations bancaires de la carte de crédit du porteur 5.

A cette étape 106, le porteur doit remplir au moins les informations concernant son emplacement physique (adresse du domicile, adresse de livraison).

L'étape 107, précédée de traits pointillés pour représenter l'intervention du tiers 6, montre qu'on a à ce niveau un choix. Le choix est de savoir si le porteur 5 s'est inscrit préalablement auprès d'un registre compris dans les moyens 600 du tiers 6, ou s'il ne s'est pas préalablement inscrit ou déclaré auprès dudit tiers 6.

Cette inscription auprès du tiers consiste notamment en la transmission des informations bancaires concernant la carte du crédit du porteur 5.

Ces informations bancaires sont notamment le numéro de carte bancaire, ainsi que la date d'échéance de la validité de la carte de crédit du porteur 5.

L'étape 108 montre le cas où le porteur 5 s'est effectivement déclaré préalablement auprès du tiers 6.

L'étape 109 montre le cas où le porteur 5 ne s'est pas préalablement déclaré auprès du tiers 6.

On rappelle que les étapes 100 à 109 constituent les étapes successives de la première étape principale 1 de la figure 1, à savoir la commande du produit.

La figure 3 part des étapes 108 et 109 et détaille les différentes étapes successives de la deuxième grande étape de la transaction financière représentée à la figure 1, à savoir le paiement de la commande.

Une première partie de la figure 3 montre qu'à partir de l'étape 108, à savoir le cas où le porteur 5 s'est préalablement déclaré auprès du tiers 6, on effectue alors une étape 200 selon laquelle le porteur 5 ne remplit que succinctement les champs concernant les informations bancaires de la carte de crédit.

Il peut alors par exemple ne remplir le champ concernant le numéro de sa carte de crédit ou la date d'échéance de validité de ladite carte de

crédit que par un identifiant auprès du tiers 6. Cet identifiant peut être un mot de passe, un code chiffré, ou les coordonnées téléphoniques auxquelles on peut joindre le porteur 5 (coordonnées de téléphone mobile par exemple).

L'étape 201 consiste à vérifier la volonté du porteur 5 à effectuer la transaction financière avec le marchand 7.

Plusieurs procédés de vérification de la volonté du porteur 5 sont possibles.

Une première possibilité est de rappeler le porteur 5 sur son téléphone mobile, le porteur 5 signifiant alors son accord d'effectuer la transaction bancaire au tiers 6 par la saisie d'un mot de passe sur son clavier de téléphone portable, cette saisie étant renvoyée directement vers les moyens 600 du porteur 6 ou à travers un petit message sur téléphonie mobile, short message service (SMS) selon la terminologie anglo-saxonne généralement utilisée.

Le message en retour du téléphone mobile devra également comporter une signature électronique.

Une deuxième possibilité de vérification de la volonté du porteur 5 peut être également de forcer le porteur 5 à saisir dans une fenêtre sécurisée apparaissant sur ses moyens 500 un mot de passe spécifique.

Une troisième possibilité est d'envoyer vers les moyens 500 du porteur 5 un courrier électronique, le porteur 5 devant alors renvoyer le courrier électronique avec un identifiant permettant de confirmer la transaction.

Enfin, on peut vérifier la signature électronique de moyens que possède le porteur 5, par exemple une carte à puce, cette carte à puce étant entrée dans des moyens de lecture spécifiques reliés au réseau de télécommunication 9.

Une fois que la volonté du porteur 5 est vérifiée, l'étape 202 consiste au remplissage du formulaire de commande par le tiers 6 à l'aide de numéros et d'informations bancaires temporaires et cohérentes afin que le marchand 7 croie que ces informations bancaires sont les réelles informations bancaires du porteur 5.

On reprend maintenant l'analyse à partir de l'étape 109, à savoir quand le porteur 5 ne s'est pas déclaré auprès du tiers 6.

A l'étape 203, le porteur 5 est obligé de remplir le formulaire de commande fourni par le site du marchand 7 à l'aide des informations bancaires de sa carte de crédit.

L'étape 204 consiste alors au remplissage par le tiers 6 des champs concernant les informations bancaires du porteur 5 par des informations bancaires temporaires et cohérentes.

A la fin des étapes 202 et 204, le bon de commande fourni par le marchand 7 est donc rempli avec des informations bancaires temporaires.

Ces informations temporaires sont donc complètement différentes de celles de la carte de crédit du porteur, mais apparaissent cohérentes au yeux d'un organisme bancaire.

L'étape 205, commune aux deux procédures à partir des étapes 108 et 109, consiste en l'envoi du bon de commande modifié vers le site du marchand 7.

A L'étape 206 le [illegible] s'il le désire envoyer ces informations temporaires à un centre d'autorisation auprès de sa banque. Dans tous les cas, on arrive à l'étape 207.

L'étape 207 et le circuit bancaire visible à la figure 8 montrent alors que la demande d'autorisation bancaire revient au centre d'autorisation du tiers 6. Ce centre d'autorisation 602 est relié au moyen 600 du tiers 6 par des moyens de traitement 601.

Lors de l'étape 208, le tiers 6 procède à une reconversion des numéros temporaires en les véritables numéros ou informations bancaires du porteur 5.

L'étape 209 consiste en l'envoi d'une demande d'autorisation de la transaction financière auprès du centre d'autorisation de la banque 8 du porteur 5.

Une fois cette autorisation obtenue, lors de l'étape 210, la banque du porteur 8 renvoie l'autorisation vers le tiers 6, qui effectue à l'étape 211 une reconversion des véritables informations bancaires en les informations temporaires du porteur 5.

Ces différentes reconversions sont effectuées par les moyens 601 du tiers 6.

L'étape 212 consiste à envoyer l'autorisation vers le centre d'autorisation de la banque du commerçant, cette étape n'étant présente que si l'étape 206 l'est également.

A la fin de l'étape 212, le centre d'autorisation du commerçant a obtenu l'autorisation de la transaction bancaire.

L'étape 300 consiste à envoyer cette autorisation de la transaction vers le site du marchand 7.

On entre donc alors dans la première étape de la troisième grande étape 3 de la transaction financière visible à la figure 1, à savoir la finalisation de la commande et les informations concernant la livraison.

A l'étape 301, le site du marchand 7 édite un bon de livraison et l'envoie vers le porteur 5. Ce bon de livraison confirme alors que la transaction a bien été effectuée, les différentes autorisations de transaction ayant été obtenues.

Les échanges entre l'étape 301 et 302 montrent que le tiers 6 contrôle encore une fois ces informations.

L'étape 303 montre la fin de la transaction financière.

Les différentes étapes sont reprises schématiquement à la figure 6. On y retrouve les différents allers et retours entre le porteur 5, le tiers 6, le marchand 7 et la banque du porteur 8.

La figure 7 reprend sous forme schématique quelques étapes visibles à la figure 6.

On y distingue notamment les moyens 700 du commerçant 7, les moyens 600, 601 et 602 du tiers 6.

Les moyens 601 sont notamment utilisés pour la conversion et reconversion des numéros d'informations bancaires en les informations temporaires.

Les moyens 602 comportent le centre d'autorisation reliées au tiers 6.

Les moyens 500 de navigation du porteur 5 sont également visibles sur cette figure.

La figure 8 est une vue schématique représentant certaines étapes des figures 2 à 4, et notamment le circuit bancaire dans son ensemble. Le centre d'autorisation de la banque du marchand 7 est également représenté, ce qui se traduit sur les schéma-blocs de la figure 3 par la présence des étapes 206 et 212.

La figure 8 représente notamment une variante de l'invention, cette variante sera décrite de façon plus détaillée dans la suite de la présente description.

La figure 5 représente une série d'étapes qui sont effectuées postérieurement à la conclusion de la transaction financière, et de façon éventuellement décorrélée.

Lors d'une première étape 400, le marchand 7 collecte via son centre de télécollecte l'ensemble des transactions qui ont été effectuées sur le réseau de télécommunication, pendant une période donnée avec des porteurs 5.

La collecte est effectuée en fonction des différents tiers 6, à savoir que le centre de collecte du marchand 7 effectue un groupe de collecte par tiers donné.

L'étape 401 consiste en la réception par les tiers 6 de l'ensemble des transactions effectuées pendant la période donnée avec les différents porteurs 5.

L'étape 402 consiste en une reconversion par les tiers de l'ensemble des informations temporaires - informations temporaires qui sont les seules auxquelles le marchand a toujours eu accès - en les véritables informations bancaires des différents porteurs.

L'étape 403 consiste à l'envoi des différents numéros et informations bancaires vers les établissements bancaires des différents porteurs 5, afin que le marchand 7 soit effectivement payé.

La figure 8 décrit plus précisément une variante selon l'invention.

Selon cette variante, le tiers 6 (comportant les moyens 600 à 602) est complété par un module Profil du Client en Banque 800 (PCB) qui est compris sur le centre d'autorisation du porteur.

Une liaison sécurisée 10 est établie entre le centre d'autorisation du porteur 8 et le centre d'autorisation 602 relié au tiers.

Le module Profil du Client en Banque 800 reçoit par cette liaison sécurisée 10 les demandes d'autorisation bancaires issues du centre d'autorisation 602.

Une interdiction de l'acquittement d'une transaction effectuée par le porteur par réseau de télécommunication est entrée par défaut dans le centre 8 d'autorisation du porteur.

Le centre d'autorisation 602 relié au tiers configure lors de l'étape 801 le module PCB pour qu'il donne au centre 8 d'autorisation du porteur 5 des informations pour le déblocage, transaction par transaction, de cette interdiction en fonction d'étapes de questionnement étape 802 sur l'autorisation d'une transaction financière.

L'étape 802 de questionnement est consécutive à une demande d'autorisation selon l'étape 209. L'étape 209 est effectuée une fois que le module PCB a été configuré lors de l'étape 801.

Les transactions par réseau de télécommunication sont déverrouillées les unes après les autres de façon individuelle.

Ensuite, les étapes de questionnement 802 du module PCB est suivi d'une autorisation de déblocage 803 vers le centre d'autorisation 8 du porteur 5.

On reprend alors le cours normal des étapes, telles que présentées 1 à 7.

L'ajout de ce module PCB 800 en association avec le centre d'autorisation 602 relié au tiers augmente grandement la sécurité des transactions.

Lorsque le centre d'autorisation de la banque du porteur fait appel au PCB (Profil Client en Banque), celui-ci effectue un certain nombre de contrôles complémentaires liés aux caractéristiques de pré-autorisation. A l'issue des contrôles, le PCB autorise ou n'autorise pas la transaction financière.

Par exemple, lorsque la transaction financière est réalisée à l'aide de la puce de la carte bancaire ou est issue d'un traitement de carte bancaire

par un distributeur automatique de billets, le centre d'autorisation de la banque du porteur poursuit ses traitements habituels sans faire appel au PCB.

Par contre, lorsque la transaction financière n'est pas réalisée à l'aide de la puce de la carte ou n'est pas issue d'un traitement de la carte bancaire dans un distributeur automatique de billets, le centre d'autorisation de la banque porteur fait appel au PCB.

Cette méthode d'utilisation du module PCB est par exemple décrite par la demande de brevet N° 01 01453.

On rappelle que le procédé selon l'invention peut avantageusement être complété en permettant à la banque du porteur :

- d'offrir des crédits en ligne lorsque le montant de la transaction s'avère important,
- de développer une véritable relation client en instituant le passage par la banque à domicile (mise à disposition d'informations sur la banque par exemple),
-de gérer d'autres produits liés au client (paiement différé par exemple, ouverture d'un compte spécialisé Internet, etc.).

On rappelle également que la description qui précède a décrit préférentiellement un liaison sécurisée du type SSL entre le porteur et le tiers, ainsi qu'entre le marchand et le tiers, mais on peut envisager une liaison sécurisée d'un autre type ou non sécurisée entre le porteur et le tiers et/ou entre le tiers et le marchand, notamment lorsque le terminal du porteur est un téléphone mobile.

REVENDICATIONS.

1. Procédé de sécurisation de transactions par carte de crédit entre un porteur (5) et un marchand (7), notamment à travers un réseau de télécommunication (9), en entrant dans le formulaire de commande fourni par le marchand (7), lors de la phase de paiement de la transaction, des informations temporaires cohérentes avec les informations bancaires de la carte du porteur (5), ces informations temporaires étant ensuite collectées par un centre d'autorisation de la transaction afin d'être mises en relation avec les véritables informations bancaires de la carte du porteur pour l'acquittement de la commande par le porteur (5) au bénéfice du marchand (7), caractérisé en ce qu'il comporte les étapes selon lesquelles :

- le porteur (5) signifie à un tiers (6) son intention d'entrer en contact avec le marchand (7) ;
- le porteur (5) entre en contact avec le marchand (7) par l'intermédiaire du tiers ;
- le tiers (6) établit une liaison entre lui et le porteur (5), ainsi qu'entre lui et le marchand (7) ;
- le tiers (6) gère la formation d'informations temporaires, l'entrée de ces informations dans le formulaire de commande ainsi que la mise en relation des informations temporaires et des véritables informations bancaires de la carte de crédit du porteur pour contrôler les différentes autorisations auprès des banques pour l'acquittement de la commande.

2. Procédé selon la revendication 1, caractérisé en ce que la liaison entre le tiers (6) et le porteur (5) est sécurisée de façon à permettre au tiers d'intercepter et de contrôler toutes les informations transmises par le porteur (5) en direction du marchand (7) via le tiers, mais de façon transparente pour le porteur (5).

3. Procédé selon l'une des revendications 1 ou 2, caractérisé en ce que la liaison entre le tiers (6) et le marchand (7) est sécurisée de façon à

permettre au tiers d'intercepter et de contrôler toutes les informations transmises par le marchand (7) en direction du porteur (5) via le tiers, mais de façon transparente pour le porteur (5).

4. Procédé selon la revendication 2, caractérisé en ce que la liaison sécurisée entre le porteur (5) et le tiers (6) est du type Couche d'Interface de connexion sécurisée.

5. Procédé selon la revendication 3, caractérisé en ce que la liaison sécurisée entre le marchand (7) et le tiers (6) est du type Couche d'Interface de connexion sécurisée.

6. Procédé selon l'une des revendications 1 à 5, caractérisé en ce que le porteur (5) signifie son intention d'entrer en contact avec le marchand (7) en effectuant une connexion sur le site du tiers et/ou en indiquant l'adresse Internet du tiers (6) dans un navigateur de réseau de télécommunication.

7. Procédé selon l'une des revendications 1 à 6, caractérisé en ce que le tiers (6) modifie les adresses Internet relatives ou absolues du site du marchand (7) pour contraindre le navigateur du porteur à lui transmettre systématiquement toutes les informations en provenance du porteur (5) vers le marchand (7).

8. Procédé selon l'une des revendications 1 à 7, caractérisé en ce que le tiers modifie les adresses Internet relatives ou absolues du site du marchand (7) pour contraindre le navigateur du marchand à lui transmettre systématiquement toutes les informations en provenance du marchand (7) vers le porteur (5).

9. Procédé selon l'une des revendications 1 à 8, caractérisé en ce que deux procédures d'acquittement de la commande sont possibles en fonction de l'inscription préalable ou non du porteur (5) auprès du

tiers (6), cette inscription comprenant la transmission audit tiers des informations bancaires concernant le porteur et sa carte de crédit dans un registre du tiers.

10. Procédé selon la revendication 9, caractérisé en ce que si le porteur (5) s'est préalablement inscrit auprès du tiers (6), il peut choisir de ne pas indiquer dans le domaine réservé du bon de commande de la transaction les informations bancaires le concernant, et par conséquent ne remplir ledit domaine que par un identifiant auprès du tiers, le remplissage de la partie nécessitant des informations bancaires étant effectué par le tiers avec des informations temporaires et cohérentes, seules ces informations temporaires étant envoyées au marchand (7).

11. Procédé selon l'une des revendications 1 à 10, caractérisé en ce qu'on déclenche une procédure de vérification de la volonté du porteur d'effectuer la transaction.

12. Procédé selon la revendication 11, caractérisé en ce que la vérification comporte une étape selon laquelle on rappelle le porteur (5) sur son téléphone mobile, le porteur signifiant son accord au tiers par la saisie d'un mot de passe qui peut être renvoyé grâce à un petit message sur téléphone mobile et/ou une signature électronique réalisée par le téléphone mobile.

13. Procédé selon la revendication 11, caractérisé en ce que la vérification comporte une étape selon laquelle le porteur saisit dans une fenêtre sécurisée un mot de passe sur les moyens connectés au réseau de télécommunication.

14. Procédé selon la revendication 11, caractérisé en ce que la vérification comporte une étape selon laquelle on envoie un courrier électronique au porteur, le porteur devant alors renvoyer le courrier

électronique avec un identifiant permettant de confirmer la transaction.

15. Procédé selon la revendication 11, caractérisé en ce que la vérification comporte une étape selon laquelle on vérifie la signature cryptographique de moyens que le porteur a en sa possession, notamment une carte à puce introduite dans un lecteur relié au réseau de télécommunication.

16. Procédé selon la revendication 9, caractérisé en ce que dans le cas où le porteur n'est pas inscrit auprès du tiers, il entre les informations bancaires de sa carte de crédit dans le formulaire de commande fourni par le marchand via le tiers, le tiers gérant alors le remplissage du formulaire de commande qui sera envoyé au marchand avec des informations temporaires.

17. Procédé selon l'une des revendications précédentes, caractérisé en ce qu'il comporte les étapes selon lesquelles :

- un centre d'autorisation bancaire (602) relié au tiers (6) collecte la demande d'autorisation bancaire en provenance du marchand (7) ou de la banque du marchand et contenant les informations temporaires ;
- ledit centre d'autorisation bancaire effectue une reconversion mettant en relation les informations temporaires et les véritables informations bancaires ;
- il envoie les véritables informations bancaires du porteur au centre d'autorisation bancaire du porteur ;
- il récupère la réponse en provenance du centre d'autorisation bancaire du porteur contenant les véritables informations bancaires ;
- il effectue une reconversion pour mettre à nouveau en relation les véritables informations bancaires et les informations temporaires ;
- il renvoie au marchand ou au centre d'autorisation de la banque du marchand la réponse du centre d'autorisation bancaire du porteur contenant les informations temporaires.

18. Procédé selon l'une des revendications 1 à 17, caractérisé en ce que périodiquement, le centre de collecte des transactions du marchand (7) envoie l'ensemble des transactions passées entre ledit marchand et des porteurs par l'intermédiaire du tiers vers un centre de collecte lié au tiers, le tiers effectuant de nouveau une reconversion des informations temporaires en les véritables informations bancaires des différents porteurs, le centre de collecte lié au tiers effectuant alors la redistribution des transactions vers les différents centres de collecte des banques des porteurs.

19. Procédé selon l'une des revendications 1 à 18, caractérisé en ce que le centre d'autorisation du porteur comporte en outre un module Profil du Client en Banque qui reçoit, par une liaison sécurisée, les demandes d'autorisation bancaire issues du centre d'autorisation relié [illegible] dule étant configuré par le centre de demande d'aut[illegible] tiers pour qu'il donne au centre d'autorisation du porteur des informations pour le déblocage, transaction par transaction, d'une interdiction d'acquittement des transactions effectuées par le porteur par réseau de télécommunication.

20. Procédé selon l'une des revendications 1 à 19, caractérisé en ce que les informations bancaires sont le numéro et de la date d'expiration de validité de la carte de crédit.

21. Procédé selon l'une des revendications 1 à 20, caractérisé en ce que la banque du porteur intervient lors des transactions entre le porteur et le marchand, en proposant au porteur des services se rapportant à la transaction.

22. Système de sécurisation de transactions par carte de crédit entre un porteur (5) et un marchand (7), notamment à travers un réseau de télécommunication (9), contenant des moyens étant aptes à entrer

dans le formulaire de commande fourni par le marchand, lors de la phase de paiement de la transaction, des informations temporaires cohérentes avec les informations bancaires de la carte du porteur (5), le système comportant des moyens formant centre d'autorisation de la transaction et aptes à collecter ces informations temporaires afin de les mettre en relation avec les véritables informations bancaires de la carte du porteur (5) pour l'acquittement de la commande par le porteur au bénéfice du marchand, caractérisé en ce qu'il comporte des moyens formant tiers (6) relié par le réseau (9) entre le porteur (5) et le marchand (7), le tiers comportant des moyens pour établir une liaison entre lui et le porteur, ainsi qu'entre lui et le marchand, le tiers comportant en outre des moyens pour former des informations temporaires, pour entrer des informations dans le formulaire de commande ainsi que pour mettre en relation des informations temporaires et des véritables informations bancaires de la carte de crédit du porteur pour contrôler les différentes autorisations auprès des banques pour l'acquittement de la commande.

23. Système selon la revendication 22, caractérisé en ce qu'il comporte en outre des moyens pour intercepter et contrôler toutes les informations transmises par le porteur en direction du marchand.

24. Système selon l'une des revendications 22 ou 23, caractérisé en ce qu'il comporte des moyens pour sécuriser la liaison entre le tiers et le porteur aptes à permettre au tiers d'intercepter et de contrôler toutes les informations transmises par le porteur (5) en direction du marchand (7) via le tiers, mais de façon transparente pour le porteur (5).

25. Système selon l'une des revendications 22 à 24, caractérisé en ce qu'il comporte des moyens pour sécuriser la liaison entre le tiers et le marchand aptes à permettre au tiers d'intercepter et de contrôler

toutes les informations transmises par le marchand (7) en direction du porteur (5) via le tiers, mais de façon transparente pour le porteur (5).

26. Système selon l'une des revendications 22 à 25, caractérisé en ce que la liaison sécurisée entre le porteur (5) et le tiers (6) est du type Couche d'Interface de connexion sécurisée.

27. Système selon l'une des revendications 22 à 26, caractérisé en ce que la liaison sécurisée entre le marchand (7) et le tiers (6) est du type Couche d'Interface de connexion sécurisée.

28. Système selon l'une des revendications 22 à 27, caractérisé en ce que le porteur (5) comporte des moyens aptes à établir une connexion avec le marchand (7) via une connexion sur le site du tiers et/ou aptes à entrer l'adresse Internet du tiers (6) dans un navigateur de réseau de télécommunication.

29. Système selon l'une des revendications 22 à 28, caractérisé en ce que le tiers comporte des moyens aptes à modifier les adresses Internet relatives ou absolues du site du marchand (7) et aptes à contraindre le navigateur du porteur à lui transmettre systématiquement toutes les informations en provenance du porteur vers le marchand (7).

30. Système selon l'une des revendications 22 à 29, caractérisé en ce que le tiers comporte des moyens aptes à modifier les adresses Internet relatives ou absolues du site du marchand (7) et aptes à contraindre le navigateur du marchand à lui transmettre systématiquement toutes les informations en provenance du marchand (7) vers le porteur (5).

31. Système selon l'une des revendications 22 à 30, caractérisé en ce qu'il comporte :

- des moyens formant centre d'autorisation bancaire (602) reliés au tiers et collectant la demande d'autorisation bancaire en provenance du marchand ou de sa banque et contenant les informations temporaires ;
- des moyens (601) aptes à effectuer une reconversion mettant en relation les informations temporaires et les véritables informations bancaires ;
- des moyens aptes à envoyer les véritables informations bancaires du porteur au centre d'autorisation bancaire du porteur ;
- des moyens aptes à récupérer la réponse en provenance du centre d'autorisation bancaire du porteur contenant les véritables informations bancaires ;
- des moyens aptes à effectuer une reconversion pour mettre à nouveau en relation les véritables informations bancaires et les informations temporaires ;
- des moyens aptes à renvoyer au marchand ou au centre d'autorisation de sa banque la réponse du centre d'autorisation bancaire du porteur contenant les informations temporaires.

32. Système selon l'une des revendications 22 à 31, caractérisé en ce que les moyens formant centre d'autorisation du porteur comportent en outre un module Profil du Client en Banque aptes à recevoir, par une liaison sécurisée, les demandes d'autorisation bancaire issues du centre d'autorisation relié au tiers, ce module étant apte à être configuré par le centre de demande d'autorisation relié au tiers pour qu'il donne au centre d'autorisation du porteur des informations pour le déblocage, transaction par transaction, d'une interdiction d'acquittement des transactions effectuées par le porteur par réseau de télécommunication.

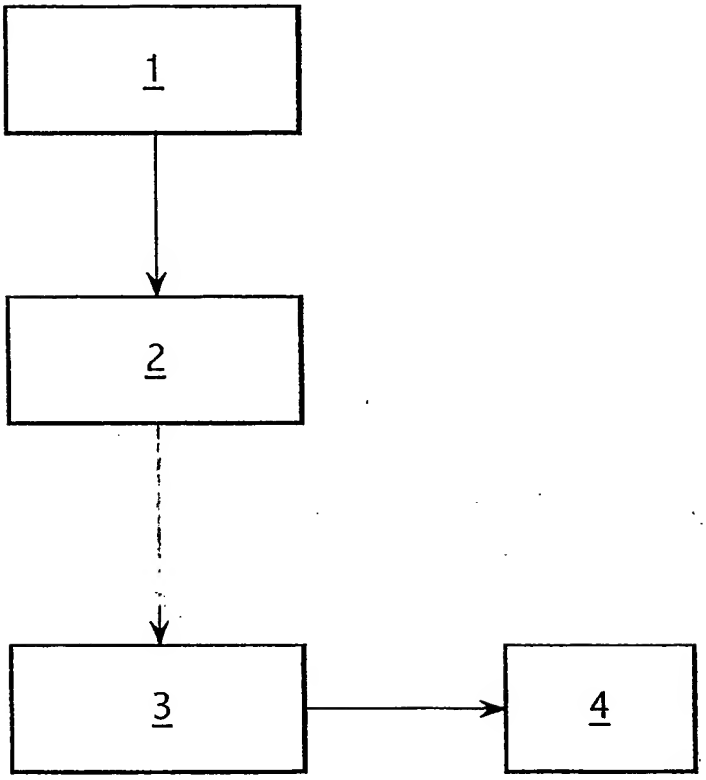


FIG.1

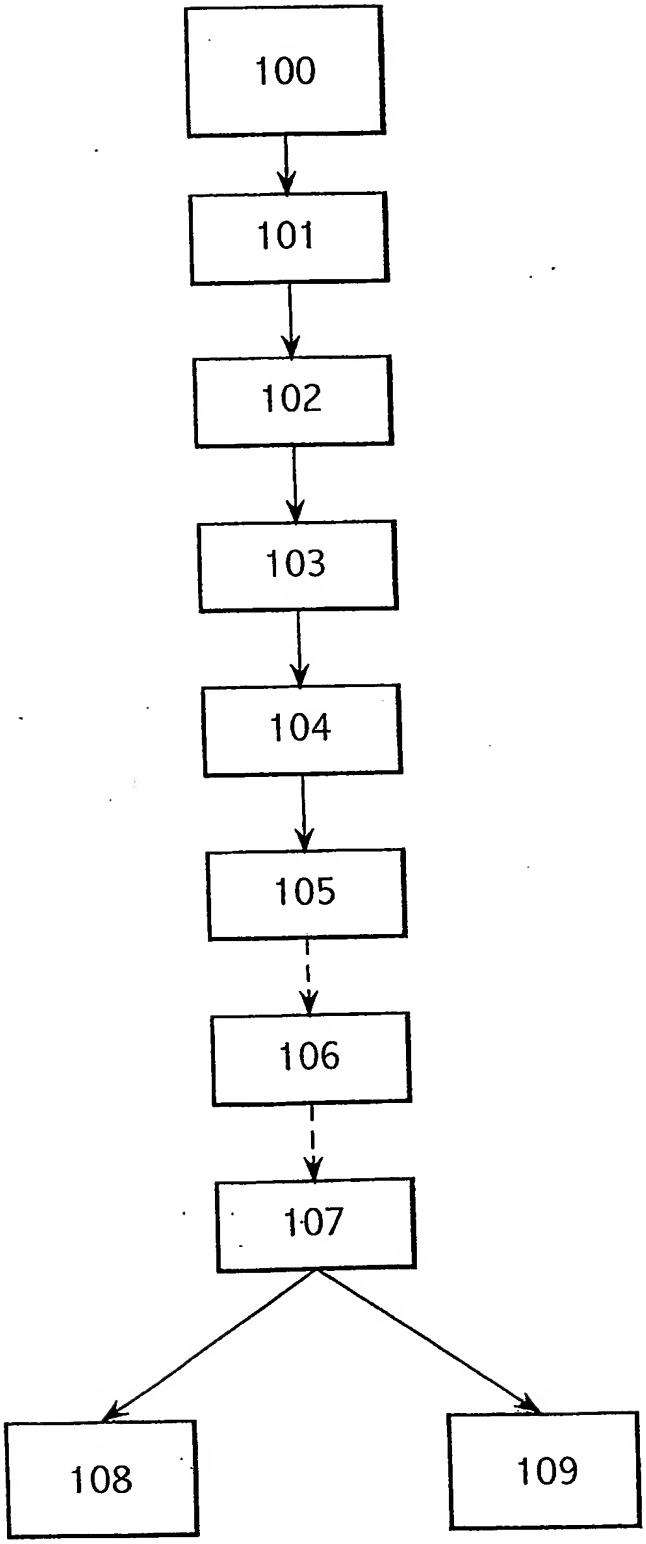


FIG.2

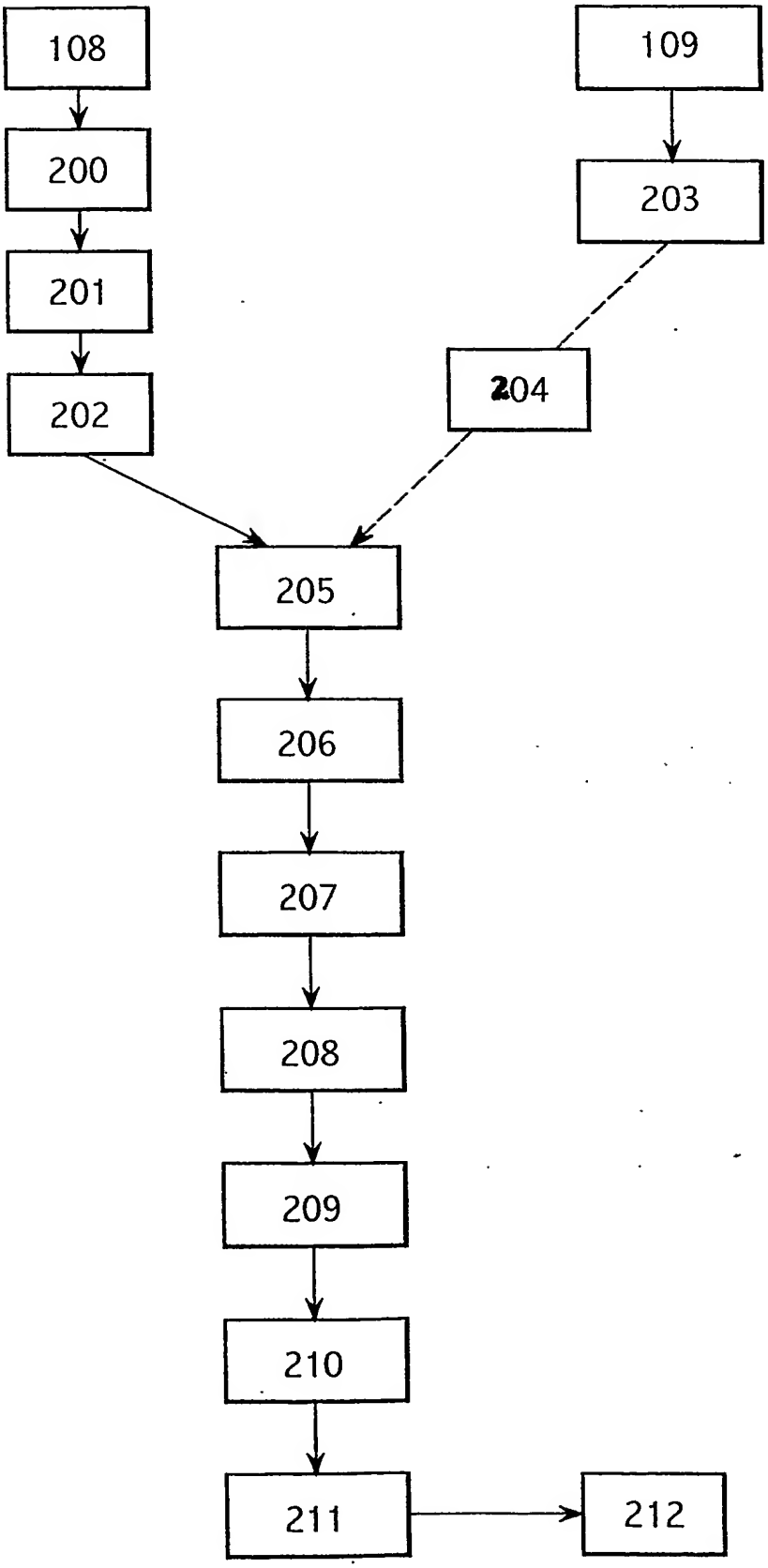


FIG.3

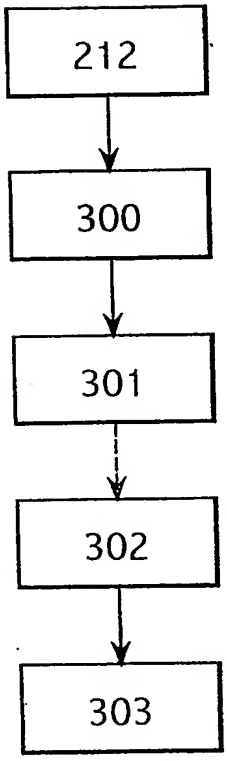


FIG.4

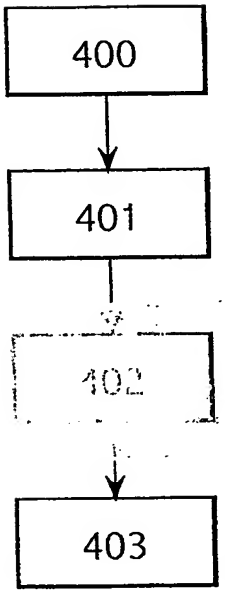


FIG.5

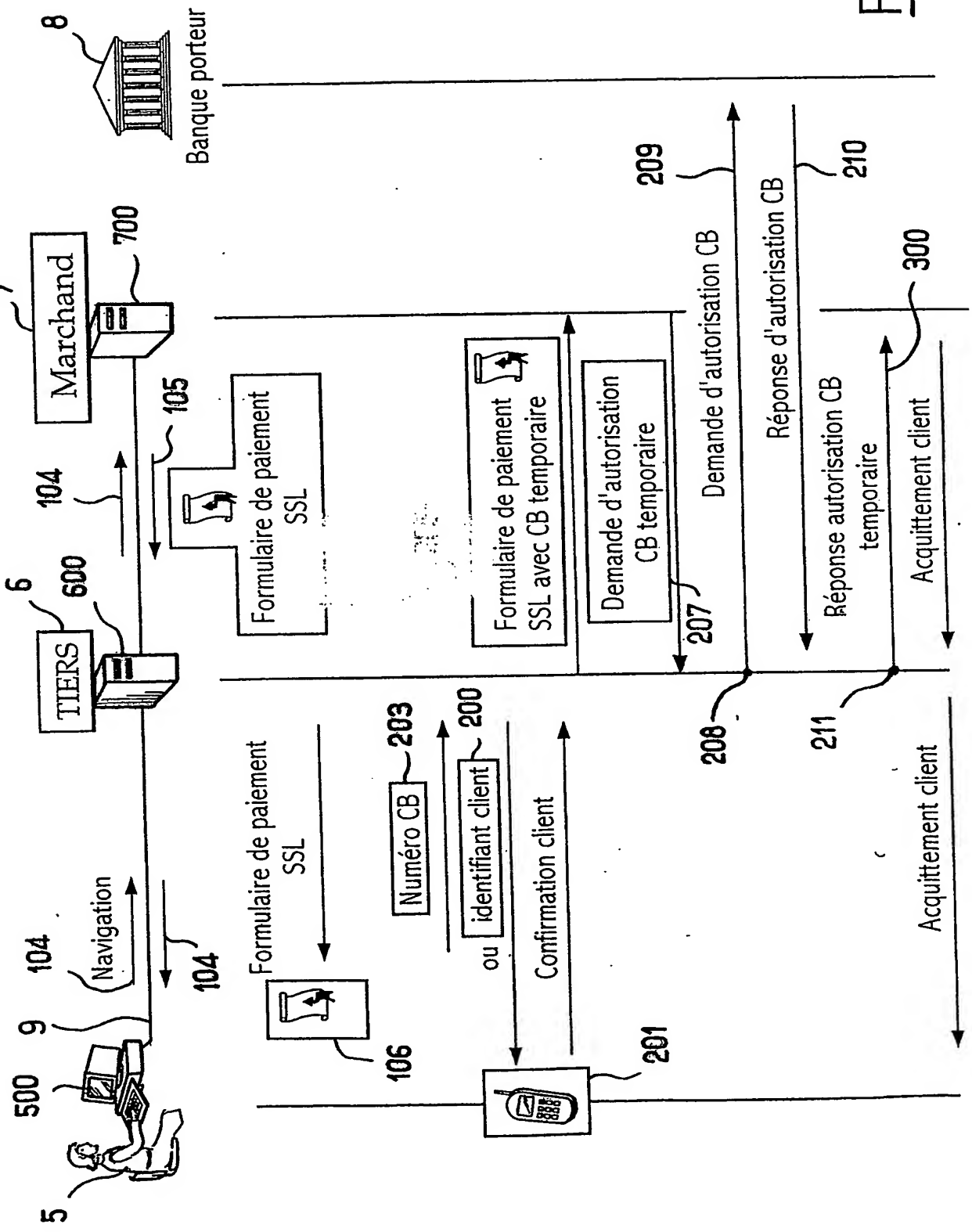

8
Banque porteur
7
Marchand
700
105
104
Formulaire de paiement SSL
6
600
TIERS
Formulaire de paiement SSL avec CB temporaire
Demande d'autorisation CB temporaire
209
Demande d'autorisation CB
207
210
Réponse d'autorisation CB
300
Réponse autorisation CB temporaire
Acquittement client
208
211
Acquittement client
Formulaire de paiement SSL
106
Numéro CB
203
ou identifiant client
200
Confirmation client
201
104
Navigation
104
9
500
5

FIG.6

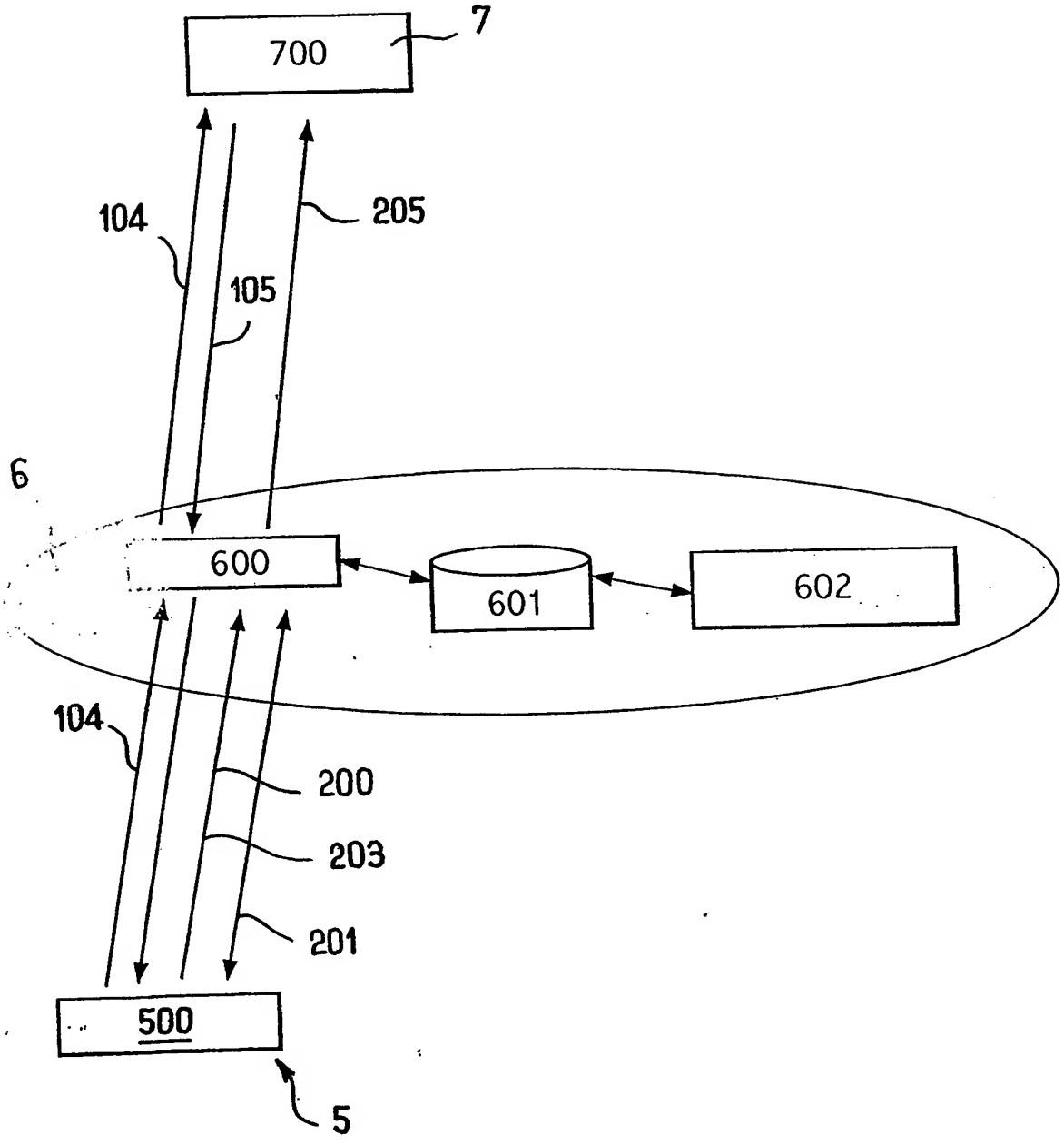


FIG.7

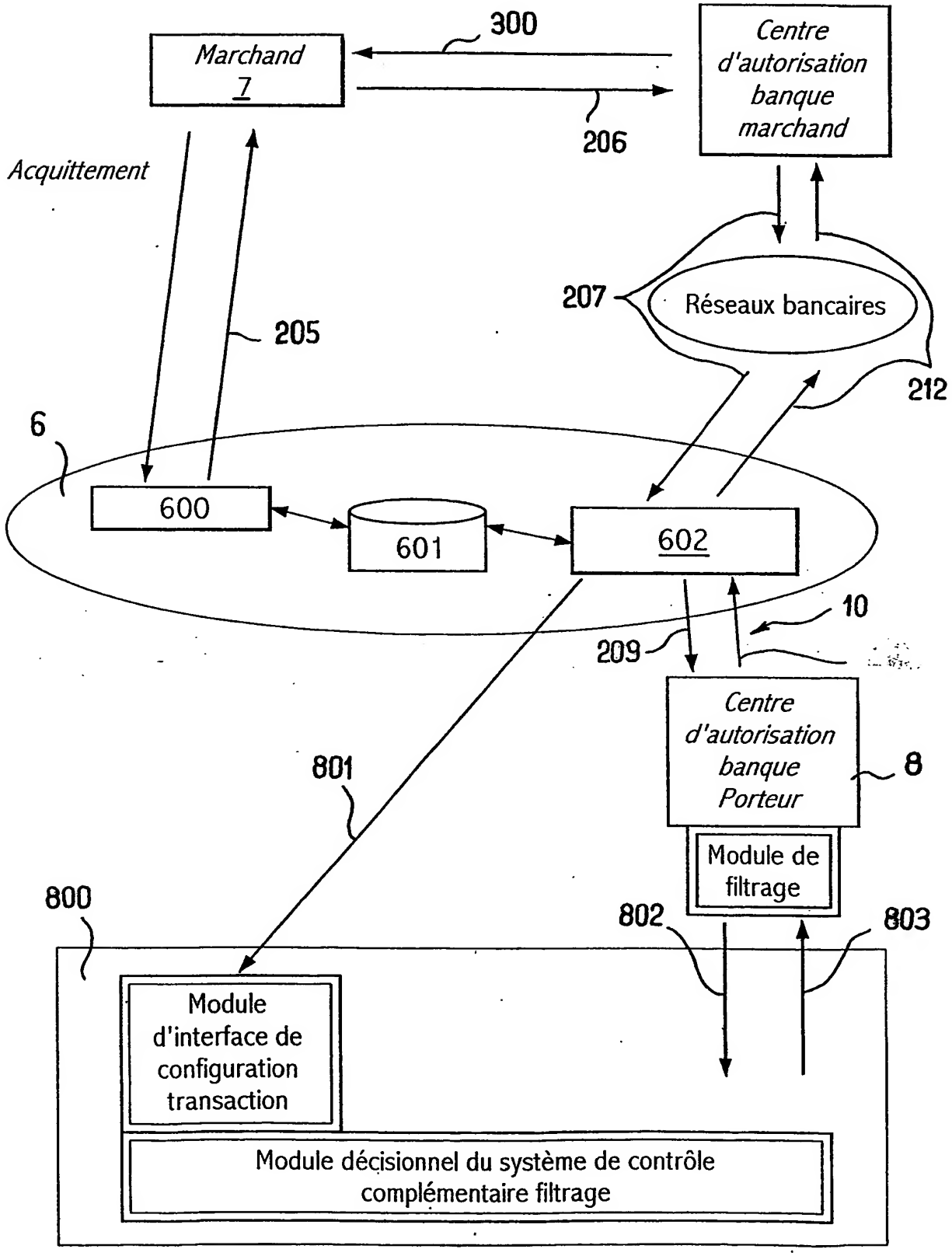

300
Marchand
7
Centre
d'autorisation
banque
marchand
206
Acquittement
205
207
Réseaux bancaires
212
6
600
601
602
10
209
Centre
d'autorisation
banque
Porteur
8
801
Module de
filtrage
800
802
803
Module
d'interface de
configuration
transaction
Module décisionnel du système de contrôle
complémentaire filtrage

FIG.8

INTERNATIONAL SEARCH REPORT

Internat Application No
PCT/. 03/00937

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 00 75749 A (INTELLISHIELD.COM, INC.) 14 December 2000 (2000-12-14)	1,6-11, 13, 16-23, 28-32
Y	page 2, line 7 - line 10 page 4, line 20 -page 7, line 26 page 8, line 22 -page 16, line 15; figures 1,3-10	2-5,12, 14,15, [illegible]-27
Y	US 5 991 738 A (OGRAM) 23 November 1999 (1999-11-23)	2,3,24, 25
A	column 1, line 49 -column 3, line 22 column 3, line 46 -column 6, line 12; figure 2E	1,22

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 July 2003	05/08/2003

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Rivero, C

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/FR 03/00937

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 01 80190 A (CYBERUN CANADA CORP.) 25 October 2001 (2001-10-25)	4,5,12, 14,15, 26,27
A	page 33, line 12 -page 46, line 7 page 152, line 16 -page 167, line 9; figures 1,2,13	1,22
A	WO 02 05231 A (PAYPAL, INC.) 17 January 2002 (2002-01-17) page 1, line 29 -page 3, line 5 page 4, line 9 -page 6, line 4; figures 1-3	1,22
A	WO 01 08066 A (IPRIVACY LLC) 1 February 2001 (2001-02-01) page 9, line 33 -page 35, line 16 page 52, line 4 -page 70, line 7; figures 1-12	1,22
A	EP 1 026 644 A (APPAGE CORPORATION) 9 August 2000 (2000-08-09) column 9, line 6 -column 16, line 56; figures 1-14	1,22

INTERNATIONAL SEARCH REPORT

Internal Application No
PCT/FR 03/00937

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 0075749 A	14-12-2000	AU 5475500 A	28-12-2000
		AU 5729200 A	28-12-2000
		WO 0075843 A1	14-12-2000
		WO 0075749 A2	14-12-2000
US 5991738 A	23-11-1999	US 5822737 A	13-10-1998
		US 2002096565 A1	25-07-2002
		US 5963917 A	05-10-1999
		US 6381584 B1	30-04-2002
WO 0180190 A	25-10-2001	CA 2305249 A1	14-10-2001
		AU 4819801 A	30-10-2001
		WO 0180190 A1	25-10-2001
		CA 2405847 A1	25-10-2001
		EP 1272987 A1	08-01-2003
WO 0205231 A	17-01-2002	AU 7333401 A	21-01-2002
		CA 2411979 A1	17-01-2002
		EP 1299865 A2	09-04-2003
		WO 0205231 A2	17-01-2002
		US 2002016765 A1	07-02-2002
WO 0108066 A	01-02-2001	AU 6229000 A	13-02-2001
		WO 0108066 A1	01-02-2001
EP 1026644 A	09-08-2000	US 5903878 A	11-05-1999
		EP 1026644 A1	09-08-2000
		AU 1469299 A	03-08-2000

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No
PCT/FR 03/00937

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 7 G07F19/00 G06F17/60

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
CIB 7 G07F G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)
WPI Data, PAJ, EPO-Internal, INSPEC

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	WO 00 75749 A (INTELLISHIELD.COM, INC.) 14 décembre 2000 (2000-12-14)	1,6-11, 13, 16-23, 28-32
Y	page 2, ligne 7 - ligne 10 page 4, ligne 20 -page 7, ligne 26 page 8, ligne 22 -page 16, ligne 15; figures 1,3-10	2-5,12, 14,15, 24-27
Y	US 5 991 738 A (OGRAM) 23 novembre 1999 (1999-11-23)	2,3,24, 25
A	colonne 1, ligne 49 -colonne 3, ligne 22 colonne 3, ligne 46 -colonne 6, ligne 12; figure 2E	1,22

-/--

[X] Voir la suite du cadre C pour la fin de la liste des documents

[X] Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
28 juillet 2003	05/08/2003

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Rivero, C.

INTERNATIONAL SEARCH REPORT

Demande internationale No
PCT/FR 03/00937

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie *	Identification des documents cités, avec,le cas échéant, l'indicationdes passages pertinents	no. des revendications visées
Y	WO 01 80190 A (CYBERUN CANADA CORP.) 25 octobre 2001 (2001-10-25)	4,5,12, 14,15, 26,27
A	page 33, ligne 12 -page 46, ligne 7 page 152, ligne 16 -page 167, ligne 9; figures 1,2,13	1,22
A	WO 02 05231 A (PAYPAL, INC.) 17 janvier 2002 (2002-01-17) page 1, ligne 29 -page 3, ligne 5 page 4, ligne 9 -page 6, ligne 4; figures 1-3	1,22
A	WO 01 08066 A (IPRIVACY LLC) 1 février 2001 (2001-02-01) page 9, ligne 33 -page 35, ligne 16 page 52, ligne 4 -page 70, ligne 7; figures 1-12	1,22
A	EP 1 026 644 A (APPAGE CORPORATION) 9 août 2000 (2000-08-09) colonne 9, ligne 6 -colonne 16, ligne 56; figures 1-14	1,22

INTERNATIONAL SEARCH REPORT

Demande nationale No
PCT/FR 03/00937

Document brevet cité au rapport de recherche		Date de publication	Membre(s) de la famille de brevet(s)		Date de publication
WO 0075749	A	14-12-2000	AU	5475500 A	28-12-2000
			AU	5729200 A	28-12-2000
			WO	0075843 A1	14-12-2000
			WO	0075749 A2	14-12-2000
US 5991738	A	23-11-1999	US	5822737 A	13-10-1998
			US	2002096565 A1	25-07-2002
			US	5963917 A	05-10-1999
			US	6381584 B1	30-04-2002
WO 0180190	A	25-10-2001	CA	2305249 A1	14-10-2001
			AU	4819801 A	30-10-2001
			WO	0180190 A1	25-10-2001
			CA	2405847 A1	25-10-2001
			EP	1272987 A1	08-01-2003
WO 0205231	A	17-01-2002	AU	7333401 A	21-01-2002
			CA	2411979 A1	17-01-2002
			EP	1299865 A2	09-04-2003
			WO	0205231 A2	17-01-2002
			US	2002016765 A1	07-02-2002
WO 0108066	A	01-02-2001	AU	6229000 A	13-02-2001
			WO	0108066 A1	01-02-2001
EP 1026644	A	09-08-2000	US	5903878 A	11-05-1999
			EP	1026644 A1	09-08-2000
			AU	1469299 A	03-08-2000

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☑ FADED TEXT OR DRAWING
- ☑ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.